SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC1	Only entities within the DomainManager process space shall be permitted to perform resolve() and list() operations, effectively protecting object references from being discovered by unauthorized entities, and preventing unwanted message traffic across the CORBA bus	3.6.2.2	Test	Shall	
SEC2	The Security Architecture shall permit Secret System High traffic.	4.1.2(1)	Not Testable	Shall	
SEC3	The CS/S of the Security Architecture shall have a minimum Common Criteria rating of EAL4.	4.1.2(2)	Inspection/ Analysis	Shall	
SEC4	The INFOSEC Boundary Component of the Security Architecture (security functions outside of the CS/S) shall have a minimum Common Criteria rating of EAL3.	4.1.2(3)	Inspection/ Analysis	Shall	
SEC5	The JTR shall use only NSA certified cryptographic chips and modules for Type 1 security functions.	4.2.1(1)	Inspection/ Analysis	Shall	
SEC6	The JTR shall implement cryptographic algorithms for specific applications as determined and specified by NSA.	4.2.1(2)	Inspection/ Analysis	Shall	
SEC7	The JTR shall be implemented in accordance with Unified INFOSEC Criteria (UIC) requirements for high security cryptographic applications.	4.2.1(3)	Witness	Shall	
SEC8	The CS/S functions of the JTR shall be evaluated to a security assurance level above EAL 4.	4.2.1(4)	Inspection/ Analysis	Shall	
SEC9	The JTR shall be implemented according to the system requirements of the UIC to include TEMPEST, tamper protection, and power requirements.	4.2.1(5)	Witness	Shall	
SEC10	Performance of ancillary cryptographic functions (e.g. algorithm decryption, authentication) shall not reduce the number of cryptographic channels available for communicator data operations.	4.2.1(6)	Test	Shall	
SEC11	The CS/S shall utilize a boot function contained within the Cryptographic Boundary.	4.2.2.2.1(1)	Inspection/ Analysis	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC12	The CS/S shall perform validity checks of data stored on non-volatile memory.	4.2.2.2.1(2)	Witness	Shall	
SEC13	The CS/S shall perform internal health tests to assure proper interconnection of objects and functionality.	4.2.2.2.1(3)	Witness	Shall	
SEC14	The CS/S shall instantiate the cryptographic algorithm decryption capability prior to waveform instantiation.	4.2.2.2.1(4)	Witness	Shall	
SEC15	The CS/S shall instantiate the key fill capability prior to waveform instantiation.	4.2.2.2.1(5)	Witness	Shall	
SEC16	The CS/S shall instantiate the key decryption capability prior to waveform instantiation.	4.2.2.2.1(6)	Witness	Shall	
SEC17	The CS/S shall instantiate the randomization capability prior to waveform instantiation.	4.2.2.2.1(7)	Witness	Shall	
SEC18	The CS/S shall perform validity checks on the cryptographic algorithm requirements (e.g., algorithm type and mode sets) provided by the CF from the waveform software profile.	4.2.2.2.2(1)	Test	Shall	
SEC19	The CS/S shall decrypt and instantiate algorithms as part of the JTR waveform instantiation process.	4.2.2.2.2(2)	Witness	Shall	
SEC20	The CS/S shall perform internal tests of instantiated algorithms prior to waveform operation.	4.2.2.2.2(3)	Test	Shall	
SEC21	The CS/S shall receive interconnection files for instantiated waveforms from the DomainManager.	4.2.2.2.2(4)	Not Testable	Shall	
SEC22	The CS/S shall accept requests for key instantiation to support a specific waveform and net application.	4.2.2.2.2(5)	Witness	Shall	
SEC23	The CS/S shall verify that there are no violations in matching classification levels of algorithms, waveforms, and keys during instantiation.	4.2.2.2.2(6)	Witness	Shall	
SEC24	The CS/S shall provide random bit stream generation to support cryptographic initialization functions.	4.2.2.2.2(7)	Witness	Shall	
SEC25	The CS/S shall perform periodic tests to assure that instantiated operations are maintained.	4.2.2.2.3(1)	Not Testable	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC26	The CS/S shall provide status outputs to authenticated requests as required.	4.2.2.2.3(2)	Test	Shall	
SEC27	The CS/S shall erase all cryptographic data memory upon cryptographic channel teardown.	4.2.2.2.4(1)	Witness	Shall	
SEC28	The CS/S shall zeroize the cryptographic channel key(s) upon channel teardown.	4.2.2.2.4(2)	Witness	Shall	
SEC29	The CS/S shall erase the cryptographic channel crypto algorithm upon user channel teardown.	4.2.2.2.4(3)	Witness	Shall	
SEC30	The CS/S shall signal channel teardown complete on status output to Audit.	4.2.2.2.4(4)	Test	Shall	
SEC31	In the event of internal failure, the CS/S shall execute internal security policy for termination or suspension of operation.	4.2.2.2.5(1)	Not Testable	Shall	
SEC32	The CS/S shall monitor external alarm and warning conditions, and execute actions according to security policy requirements.	4.2.2.2.5(2)	Not Testable	Shall	
SEC33	The CS/S shall provide failure status to Audit, if possible.	4.2.2.2.5(3)	Test	Shall	
SEC34	The CS/S shall not execute automatic retries to recover from alarm conditions.	4.2.2.2.5(4)	Witness	Shall	
SEC35	The CS/S shall accept requests for reset/retry from authenticated sources to recover from alarm conditions.	4.2.2.2.5(5)	Witness	Shall	
SEC36	The CS/S shall provide Type 1 encryption capabilities for protection of classified information.	4.2.3.2.1(1)	Witness	Shall	
SEC37	When required for a specific application, the CS/S shall encrypt software files for JTR internal storage.	4.2.3.2.1(2)	Test	Shall	
SEC38	When required for a specific application, the CS/S shall encrypt communicator data for JTR internal storage.	4.2.3.2.1(3)	Test	Shall	
SEC39	The CS/S shall encrypt keying material for JTR internal storage.	4.2.3.2.1(4)	Witness	Shall	
SEC40	The CS/S shall be able to use different encryption algorithms.	4.2.3.2.1(5)	Witness	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC41	When required for specific applications and configurations, the CS/S shall simultaneously encrypt communicator data using different cryptographic applications.	4.2.3.2.1(6)	Test	Shall	
SEC42	When required for specific applications, the CS/S shall encrypt RED side data and return the processed output to the RED side.	4.2.3.2.1(7)	Test	Shall	
SEC43	When required for specific applications, the CS/S shall encrypt BLACK side data and return the processed output to the BLACK side.	4.2.3.2.1(8)	Test	Shall	
SEC44	The CS/S shall provide Type 1 capabilities for decryption of classified information.	4.2.3.2.2(1)	Witness	Shall	
SEC45	When required for a specific application, the CS/S shall decrypt software files from JTR internal storage.	4.2.3.2.2(2)	Test	Shall	
SEC46	When required for a specific application, the CS/S shall decrypt communicator data from JTR internal storage.	4.2.3.2.2(3)	Test	Shall	
SEC47	The CS/S shall decrypt keying material from JTR internal storage.	4.2.3.2.2(4)	Witness	Shall	
SEC48	The CS/S shall be able to use different decryption algorithms.	4.2.3.2.2(5)	Witness	Shall	
SEC49	When required for specific applications and configurations, the CS/S shall simultaneously decrypt communicator data using different cryptographic applications.	4.2.3.2.2(6)	Test	Shall	
SEC50	When required for specific applications, the CS/S shall decrypt RED side data and return the processed output to the RED side.	4.2.3.2.2(7)	Test	Shall	
SEC51	When required for specific applications, the CS/S shall decrypt BLACK side data and return the processed output to the BLACK side.	4.2.3.2.2(8)	Test	Shall	
SEC52	The CS/S shall provide keystream to JTR processing functions external to the CS/S for use in TRANSEC waveform development.	4.2.3.2.3(1)	Witness	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC53	When required for a specific application, the CS/S shall use time-of-day (TOD) functions for keystream generation.	4.2.3.2.3(2)	Witness	Shall	
SEC54	The TRANSEC keystream shall be used immediately after generation, as specified as in the UIC.	4.2.3.2.3(3)	Witness	Shall	
SEC55	The TRANSEC keystream shall be distinct from the encrypt and decrypt keystreams.	4.2.3.2.3(4)	Witness	Shall	
SEC56	The CS/S shall perform cryptographically based authentication for RED messages.	4.2.4.2(1)	Witness	Shall	
SEC57	The CS/S shall perform cryptographically based authentication for BLACK messages.	4.2.4.2(2)	Witness	Shall	
SEC58	The CS/S shall return results of authentication processing to the message originating object.	4.2.4.2(3)	Witness	Shall	
SEC59	The CS/S shall provide Digital Signature Standard (DSS) cryptographic processing.	4.2.4.2(4)	Witness	Shall	
SEC60	The CS/S shall store DSS certificates.	4.2.4.2(5)	Witness	Shall	
SEC61	The CS/S shall generate DSS authentication messages.	4.2.4.2(6)	Witness	Shall	
SEC62	The CS/S shall perform cryptographically based authentication for RED messages.	4.2.5.2(1)	Witness	Shall	
SEC63	The CS/S shall perform cryptographically based authentication for BLACK messages.	4.2.5.2(2)	Witness	Shall	
SEC64	The CS/S shall return results of integrity processing to the originating object.	4.2.5.2(3)	Witness	Shall	
SEC65	The CS/S shall provide Secure Hash Algorithm (SHA-1) processing.	4.2.5.2(4)	Witness	Shall	
SEC66	The CS/S shall generate SHA-1 based integrity checks.	4.2.5.2(5)	Witness	Shall	
SEC67	6. The CS/S shall generate standard integrity checks [e.g., parity, cyclic redundancy check (CRC)] for data.	4.2.5.2(6)	Witness	Shall	
SEC68	The JTR shall accept BLACK keys using the DS-101 protocol.	4.2.6.1.2.1(1)	Witness	Shall	
SEC69	The JTR shall accept RED keys using the DS-101 protocol.	4.2.6.1.2.1(2)	Witness	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC70	The JTR shall accept DS-100-1 key tagging information.	4.2.6.1.2.1(3)	Witness	Shall	
SEC71	The JTR shall be capable of binding key tagging and ID information to a key.	4.2.6.1.2.1(4)	Witness	Shall	
SEC72	The JTR shall accept RED keys using the DS-102 protocol.	4.2.6.1.2.1(5)	Witness	Shall	
SEC73	The JTR shall accept encrypted keys using the DS-102 protocol.	4.2.6.1.2.1(6)	Witness	Shall	
SEC74	The JTR shall permit the operator/security officer to enter key identification information.	4.2.6.1.2.1(7)	Test	Shall	
SEC75	Key identification information (Tag 100-1 or optional text, e.g., "text ID") for stored keys shall be available to an authenticated user.	4.2.6.1.2.1(8)	Test	Shall	
SEC76	In a multi-channel radio environment, the CS/S shall accept black key load while other channels are operational (for local fill).	4.2.6.1.2.1(9)	Test	Shall	
SEC77	The JTR shall accept Data 100-1 key fill data information.	4.2.6.1.2.1(10)	Witness	Shall	
SEC78	The JTR shall have a benign fill capability for JTR System keys (i.e., not TEKs).	4.2.6.1.2.1(11)	Witness	Shall	
SEC79	Key storage shall be in BLACK form.	4.2.6.1.2.2(1)	Witness	Shall	
SEC80	Classified keys in RED form shall not exist outside of the Cryptographic Boundary.	4.2.6.1.2.2(2)	Inspection/ Analysis	Shall	
SEC81	Keys shall be bound to their respective identification information in storage.	4.2.6.1.2.2(3)	Witness	Shall	
SEC82	The CS/S shall encrypt developed keys for storage.	4.2.6.1.2.2(4)	Witness	Shall	
SEC83	The CS/S shall encrypt updated keys for storage.	4.2.6.1.2.2(5)	Witness	Shall	
SEC84	Keys shall be requested for use according to their tag or ID information.	4.2.6.1.2.3(1)	Test	Shall	
SEC85	The CS/S shall not permit keys to be instantiated for an improper application.	4.2.6.1.2.3(2a)	Witness	Shall	
SEC86	The CS/S shall not permit keys to be instantiated for an improper application (Using the wrong key type (e.g., TEK, KEK, TSK)	4.2.6.1.2.3(2b)	Witness	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC87	The CS/S shall not permit keys to be instantiated for an improper application (Mismatching a key with an algorithm (e.g., a KGV-11 key with a KG-84 algorithm))	4.2.6.1.2.3(2c)	Witness	Shall	
SEC88	The CS/S shall not permit keys to be instantiated for an improper application (Using the wrong compartment (e.g., US, NATO, Allied)	4.2.6.1.2.3(2d)	Witness	Shall	
SEC89	Keys shall be tested for integrity at instantiation.	4.2.6.1.2.3(3)	Witness	Shall	
SEC90	The CS/S shall permit Unclassified keys to be passed outside of the Cryptographic Boundary for specific purposes (e.g., BLACK processor generated TRANSEC, GPS).	4.2.6.1.2.3(4)	Test	Shall	
SEC91	The CS/S shall use Tamper detection keys, when required by a specific application.	4.2.6.1.2.3(5)	Witness	Shall	
SEC92	The CS/S shall use split keys, when required by a specific application.	4.2.6.1.2.3(6)	Witness	Shall	
SEC93	The CS/S shall provide token [e.g., crypto ignition key (CIK)] split generation and processing, when required by a specific application.	4.2.6.1.2.3(7)	Witness	Shall	
SEC94	When required for a specific application, the token/CIK function shall disable the classified processing capabilities of the CS/S upon token removal.	4.2.6.1.2.3(8)	Witness	Shall	
SEC95	The CIK function shall declassify the equipment (a minimum of Controlled Cryptographic Item) by removing RED keys and cryptographic algorithms.	4.2.6.1.2.3(9)	Witness	Shall	
SEC96	When required for specific applications, the CS/S shall develop keys via Firefly processing.	4.2.6.1.2.3(10)	Witness	Shall	
SEC97	The JTR shall provide a hardware mechanism for a user to zeroize all RED keys.	4.2.6.1.2.4(1)	Witness	Shall	
SEC98	The JTR shall provide a software mechanism for a user to zeroize all RED keys.	4.2.6.1.2.4(2)	Witness	Shall	
SEC99	The JTR shall provide a hardware mechanism for a user to zeroize all active key splits.	4.2.6.1.2.4(3)	Witness	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC100	The JTR shall provide a software mechanism for a user to zeroize all active key splits.	4.2.6.1.2.4(4)	Witness	Shall	
SEC101	A capability shall be provided for a user to selectively erase BLACK and RED keys.	4.2.6.1.2.4(5)	Witness	Shall	
SEC102	Remote key zeroization commands shall be cryptographically authenticated.	4.2.6.1.2.4(6)	Witness	Shall	
SEC103	Local HMI software-based zeroization commands shall be authenticated.	4.2.6.1.2.4(7)	Test	Shall	
SEC104	Legacy key update functions shall erase the prior version of the key .	4.2.6.1.2.4(8)	Witness	Shall	
SEC105	BLACK keys shall be erased as part of zeroization if power is available.	4.2.6.1.2.4(9)	Witness	Shall	
SEC106	When required for a specific application, the JTR shall generate OTAZ messages.	4.2.6.1.2.4(10)	Test	Shall	
SEC107	When required for a specific application, the JTR shall receive, authenticate, and process and respond to OTAZ messages.	4.2.6.1.2.4(11)	Witness	Shall	
SEC108	OTAZ messages shall be cryptographically authenticated.	4.2.6.1.2.4(12)	Witness	Shall	
SEC109	The CS/S shall maintain an identification file of cryptographic key holdings correlated with waveform, algorithm, and network management key data.	4.2.6.1.2.5(1)	Test	Shall	
SEC110	When audit is invoked, the CS/S shall maintain an identification file of keys loaded and keys zeroized or erased.	4.2.6.1.2.5(2)	Test	Shall	
SEC111	The CS/S shall provide information to authorized users and to the DomainManager as to which keys have expired.	4.2.6.1.2.5(3)	Test	Shall	
SEC112	The JTR shall accept keying messages over a radio (BLACK) channel using an OTAT function.	4.2.6.1.2.6(1)	Test	Shall	
SEC113	When required for a specific application, the CS/S shall develop OTAR messages for legacy interoperability.	4.2.6.1.2.6(2)	Test	Shall	
SEC114	When required for a specific application, the CS/S shall accept OTAR messages for legacy interoperability.	4.2.6.1.2.6(3)	Test	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC115	When required for a specific application, the CS/S shall perform legacy key update functions.	4.2.6.1.2.6(4)	Test	Shall	
SEC116	When required for a specific application, the CS/S shall provide key development using asymmetric vector techniques.	4.2.6.1.2.6(5)	Witness	Shall	
SEC117	OTAR messages shall be cryptographically authenticated.	4.2.6.1.2.6(6)	Witness	Shall	
SEC118	OTAT messages shall be cryptographically authenticated.	4.2.6.1.2.6(7)	Witness	Shall	
SEC119	The CS/S shall not generate keys for external communications use.	4.2.6.1.2.6(8)	Witness	Shall	
SEC120	When required for a specific application, the CS/S shall generate key splits to update token-based functions.	4.2.6.1.2.6(9)	Witness	Shall	
SEC121	All classified cryptographic algorithms shall be decrypted using the JOSEKI-1 algorithm.	4.2.6.2.2.1(1)	Witness	Shall	
SEC122	CS/S shall only accept cryptographic algorithms/algorithm packages signed by NSA.	4.2.6.2.2.1(2)	Witness	Shall	
SEC123	The CS/S shall perform authentication and integrity checks of received algorithms or algorithm packages.	4.2.6.2.2.1(3)	Witness	Shall	
SEC124	The CS/S shall report the results of integrity checks as auditable events.	4.2.6.2.2.1(4)	Test	Shall	
SEC125	The CS/S shall not accept versions of a cryptographic algorithm or algorithm package that are older than the currently installed version.	4.2.6.2.2.1(5)	Witness	Shall	
SEC126	Cryptographic algorithms or algorithm packages shall be identified as to type and version.	4.2.6.2.2.1(6)	Witness	Shall	
SEC127	The JTR shall provide for operator/security officer entry of acceptable versions of cryptographic algorithms or algorithm packages.	4.2.6.2.2.1(7)	Test	Shall	
SEC128	The CS/S shall accept BLACK key and cryptographic downloads using the security API.	4.2.6.2.2.1(8)	Test	Shall	
SEC129	Cryptographic algorithms or algorithm packages shall be downloaded separate from other JTR non-security software.	4.2.6.2.2.2(1)	Test	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC130	The JTR shall accept cryptographic algorithms or cryptographic algorithm packages downloaded as software files using the DS-101 protocol.	4.2.6.2.2.2(2)	Test	Shall	
SEC131	Cryptographic algorithms shall be stored in BLACK form.	4.2.6.2.2.2(3)	Witness	Shall	
SEC132	Cryptographic algorithms shall be bound to their version and type identification in storage.	4.2.6.2.2.2(4)	Witness	Shall	
SEC133	The CS/S shall accept requests for cryptographic algorithm instantiation based on waveform software profile requirements.	4.2.6.2.2.3(1)	Test	Shall	
SEC134	If the cryptographic algorithm is constructed with configuration options, the CS/S shall accept control requests for cryptographic algorithm options based on waveform software profile requirements.	4.2.6.2.2.3(2)	Test	Shall	
SEC135	Instantiated cryptographic algorithms shall be tested for correct function prior to operational use.	4.2.6.2.2.3(3)	Witness	Shall	
SEC136	Instantiated cryptographic algorithms shall be erased at cryptographic channel teardown.	4.2.6.2.2.3(4)	Witness	Shall	
SEC137	In a multi-channel radio environment, the CS/S shall accept cryptographic algorithm instantiation while other channels are operational.	4.2.6.2.2.3(5)	Test	Shall	
SEC138	Old cryptographic algorithm versions shall be erased by a manual action when new algorithm versions are downloaded and verified as to authentication and integrity.	4.2.6.2.2.4(1)	Witness	Shall	
SEC139	Requirements for Zeroization of decrypt key(s) for cryptographic algorithms concurrent with traffic keys shall be design, mission, and environment dependent.	4.2.6.2.2.4(2)	Witness	Shall	
SEC140	Algorithm download events shall be stored as part of audit log functions.	4.2.6.2.2.5(1)	Test	Shall	
SEC141	Audit files for algorithm activities shall be access restricted to authenticated users or automated audit data recipients.	4.2.6.2.2.5(2)	Test	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC142	Policy rules for cryptographic bypass shall be protected either by: storage within the CS/S or using access control with integrity checks.	4.2.6.3.2(1)	Not Testable	Shall	
SEC143	The CS/S shall accept waveform security policy elements from software profiles at waveform instantiation.	4.2.6.3.2(2)	Test	Shall	
SEC144	The CS/S shall examine requested cryptographic keys for consistency of tag information (e.g., classification).	4.2.6.3.2(3)	Witness	Shall	
SEC145	The CS/S shall accept user security policy elements from authenticated HMI communications.	4.2.6.3.2(4)	Not Testable	Shall	
SEC146	The CS/S shall provide security policy status upon authenticated request.	4.2.6.3.2(5)	Not Testable	Shall	
SEC147	The CS/S internal security policy tables shall not be accessible to JTR objects external to the CS/S without authentication.	4.2.6.3.2(6)	Not Testable	Shall	
SEC148	The CS/S shall enforce the internal security policy for security critical items prior to reporting status to the OE or HMI.	4.2.6.3.2(7)	Not Testable	Shall	
SEC149	The CS/S shall decrypt Security Critical Software files from JTR internal storage.	4.2.6.5(1)	Witness	Shall	
SEC150	The CS/S shall encrypt Security Critical Software files for JTR internal storage.	4.2.6.5(2)	Witness	Shall	
SEC151	Security critical software within the CS/S shall be subject to detailed software evaluation.	4.2.6.5(3)	Witness	Shall	
SEC152	Security Critical Software that implements a cryptographic algorithm and supporting functions for keying, instantiation, and control shall be configuration controlled after evaluation.	4.2.6.5(4)	Inspection/ Analysis	Shall	
SEC153	Only software that is configuration controlled shall be implemented into JTRS-compliant equipment for security critical functions.	4.2.6.5(5)	Witness	Shall	
SEC154	The CS/S shall perform integrity checks on Security Critical Software programs and files prior to instantiation or use.	4.2.6.5(6)	Witness	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC155	The ApplicationFactory shall provide the application specific requirement of the bypass security policy to the CS/S control interface.	4.2.7.1.2(1)	Test	Shall	
SEC156	The CS/S shall control the bypass function according to the security policy.	4.2.7.1.2(2)	Witness	Shall	
SEC157	The CS/S shall provide a mechanism to terminate communication on the cryptographic channel if the bypass policy is violated.	4.2.7.1.2(3)	Test	Shall	
SEC158	Only the crypto subsystem shall provide the control/status bypass function between the RED and BLACK side of the JTR.	4.2.7.2.1(1)	Witness	Shall	
SEC159	The control/status bypass parameters shall be associated with the application requesting the bypass.	4.2.7.2.1(2)	Test	Shall	
SEC160	The control/status bypass mechanism(s) shall accept bypass policy either on a per-application basis or create a separate bypass mechanism per policy.	4.2.7.2.1(3)	Test	Shall	
SEC161	The system control control/status bypass mechanism shall be distinct from waveform control/status bypass mechanism.	4.2.7.2.1(4)	Witness	Shall	
SEC162	The control/status bypass mechanism shall be non-bypassable.	4.2.7.2.1(5)	Witness	Shall	
SEC163	The control/status bypass mechanism shall be always invoked.	4.2.7.2.1(6)	Witness	Shall	
SEC164	The control/status bypass mechanism shall be provided tamper protection.	4.2.7.2.1(7)	Witness	Shall	
SEC165	Covert channel analysis shall be performed on the bypass channel.	4.2.7.2.1(8)	Witness	Shall	
SEC166	The control/status bypass mechanism shall output all violations of bypass security policy to the Audit Function.	4.2.7.2.1(9)	Test	Shall	
SEC167	The bypass mechanism shall block messages that violate the bypass security policy.	4.2.7.2.1(10)	Witness	Shall	
SEC168	Bypass messages that violate the bypass policy shall not be transmitted.	4.2.7.2.1(11)	Witness	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC169	If policy violation exceeds a policy-determined threshold, the bypass channel shall be closed, resulting in termination of the operation of the affected channel.	4.2.7.2.1(12)	Witness	Shall	
SEC170	When required for a specific application, the control/status bypass mechanism algorithm shall check for valid connections between objects.	4.2.7.2.1(13)	Test	Shall	
SEC171	When required for a specific application, the control/status bypass mechanism algorithm shall check for valid format of bypass messages.	4.2.7.2.1(14)	Test	Shall	
SEC172	When required for a specific application, the control/status bypass mechanism algorithm shall check for valid length of bypass message.	4.2.7.2.1(15)	Test	Shall	
SEC173	When required for a specific application, the control/status bypass mechanism algorithm shall check for valid frequency of bypass messages for a given bypass mechanism.	4.2.7.2.1(16)	Test	Shall	
SEC174	The bypass algorithm requirements shall be contained in the bypass policy that is downloaded to the bypass mechanism.	4.2.7.2.1(17)	Test	Shall	
SEC175	The bypass policy shall be protected either by storage in the cryptographic boundary or by using access controls and integrity checks.	4.2.7.2.1(18)	Test	Shall	
SEC176	The format of the policy that is downloaded shall be eXtensible Mark-up Language (XML).	4.2.7.2.1(19)	Test	Shall	
SEC177	The CS/S shall accept control messages only from proper sources external to the CS/S.	4.2.8.2(1)	Not Testable	Shall	
SEC178	The CS/S shall accept requests only from the proper sources external to the CS/S.	4.2.8.2(2)	Not Testable	Shall	
SEC179	The CS/S shall accept files from the OE that define the waveform interconnections as instantiated by the CF	4.2.8.2(3)	Not Testable	Shall	
SEC180	The CS/S shall internally store files that define the waveform interconnections as instantiated by the CF.	4.2.8.2(4)	Not Testable	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC181	When Required for a specific application, the CS/S will perform health checks during run-time operation of a waveform that verifies the accuracy of the instantiated waveform interconnections.	4.2.8.2(5)	Test	Shall	
SEC182	The CS/S shall provide status messages and alarms to the Audit function.	4.2.8.2(6)	Test	Shall	
SEC183	The CS/S shall be a Consumer for alarms generated within the JTR.	4.2.8.2(7)	Test	Shall	
SEC184	The CS/S shall maintain a security policy to determine responses to alarms generated internal to the CS/S.	4.2.8.2(8)	Witness	Shall	
SEC185	The CS/S shall maintain a security policy to determine responses to alarms generated external to the CS/S.	4.2.8.2(9)	Not Testable	Shall	
SEC186	A JTRS implementation shall provide process separation when processing classified/sensitive data.	4.3.2.2(1)	Inspection/ Analysis	Shall	
SEC187	A JTRS implementation shall provide process separation when performing security critical functions.	4.3.2.2(2)	Inspection/ Analysis	Shall	
SEC188	A JTRS implementation shall provide process separation between OS, CF, and application(s).	4.3.2.2(3)	Inspection/ Analysis	Shall	
SEC189	The process separation mechanism shall provide controlled methods of transfer from one process to another.	4.3.2.2(4)	Inspection/ Analysis	Shall	
SEC190	The process separation shall be implemented by a combination of hardware and/or software.	4.3.2.2(5)	Inspection/ Analysis	Shall	
SEC191	The software portion of the process separation implementation shall exist within the operating system.	4.3.2.2(6)	Inspection/ Analysis	Shall	
SEC192	The process separation mechanism shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures).	4.3.2.2(7)	Inspection/ Analysis	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC193	The process separation mechanism shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.	4.3.2.2(8)	Inspection/ Analysis	Shall	
SEC194	An entity shall define and control access between named users and named objects.	4.3.3.2(1)	Inspection/ Analysis	Shall	
SEC195	The enforcement mechanism shall allow users to specify and control sharing of those objects by named individuals.	4.3.3.2(2)	Inspection/ Analysis	Shall	
SEC196	The enforcement mechanism shall provide controls to limit propagation of access rights.	4.3.3.2(3)	Inspection/ Analysis	Shall	
SEC197	The access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access.	4.3.3.2(4)	Inspection/ Analysis	Shall	
SEC198	Access controls shall be capable of including or excluding access to a single user.	4.3.3.2(5)	Test	Shall	
SEC199	Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.	4.3.3.2(6)	Inspection/ Analysis	Shall	
SEC200	The access control mechanism shall exist in a domain separate from user applications that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the entity may be a defined subset of the subjects and objects in the processing system.	4.3.3.2(7)	Inspection/ Analysis	Shall	
SEC201	The access control mechanism shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.	4.3.3.2(8)	Inspection/ Analysis	Shall	
SEC202	An entity shall require users to identify themselves to it before performing any other actions that the entity is expected to mediate.	4.3.4.2(1)	Test	Shall	
SEC203	Furthermore, the entity shall use a protected mechanism (e.g., passwords) to authenticate the user's identity.	4.3.4.2(2)	Test	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC204	The entity shall protect authentication data so that any unauthorized user cannot access it.	4.3.4.2(3)	Test	Shall	
SEC205	The entity shall be able to enforce individual accountability by providing the capability to uniquely identify each individual system user.	4.3.4.2(4)	Test	Shall	
SEC206	The entity shall provide the capability of associating this identity with all auditable actions taken by that individual.	4.3.4.2(5)	Test	Shall	
SEC207	All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the entity's pool of unused storage objects.	4.3.5.2(1)	Inspection/ Analysis	Shall	
SEC208	The JTR shall clear all memory used to store classified traffic prior to instantiating lower classifications of system high.	4.3.5.2(2)	Inspection/ Analysis	Shall	
SEC209	The JTR shall clear all memory used to store classified traffic prior to instantiating channels of different system high type classification.	4.3.5.2(3)	Witness	Shall	
SEC210	Access to cryptographic interfaces shall be restricted only to objects with the appropriate authorization (permissions).	4.3.7.1.2(1)	Not Testable	Shall	
SEC211	Security APIs shall be implemented in accordance with Attachment A:Security Application Program Interface Service Definition.	4.3.7.1.2(2)	Test	Shall	
SEC212	Security APIs shall be used to control/access all Cryptographic Services by other software objects within the JTR Set.	4.3.7.1.2(3)	Test	Shall	
SEC213	The Security APIs shall use the Cryptographic Service Building Blocks.	4.3.7.1.2(4)	Test	Shall	
SEC214	The HMI transport utilized shall be independent of other transports that are used to communicate between internal JTR objects.	4.3.7.2.2(1)	Inspection/ Analysis	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC215	Internal message protocols stacks and host interface message protocol stacks shall reside in separate process space.	4.3.7.2.2(2)	Inspection/ Analysis	Shall	
SEC216	The security policy associated with the HMI security policy enforcement guard shall be tailored specifically for operator, administrator, security operator, maintainer, or communicator (as a systems application or SAP).	4.3.7.2.2(3)	Test	Shall	
SEC217	The security policy shall be loaded during the application instantiation.	4.3.7.2.2(4)	Not Testable	Shall	
SEC218	A unique instantiation of the security policy enforcement mechanism shall be used for each host interface.	4.3.7.2.2(5)	Not Testable	Shall	
SEC219	The associated security policy shall identify an individual's legitimate permissions within the system.	4.3.7.2.2(6)	Test	Shall	
SEC220	If high assurance host authentication is required (e.g., remote control requirement), the HMI security policy enforcement mechanism shall use the Security API for the Integrity/Authentication cryptographic service.	4.3.7.2.2(7)	Witness	Shall	
SEC221	The CF shall be checked for file integrity prior to instantiation.	4.3.7.3.2(1)	Inspection/ Analysis	Shall	
SEC222	Cryptographic Services of the JTR shall be active prior to the ability of the CF to instantiate waveforms.	4.3.7.3.2(2)	Test	Shall	
SEC223	The installer application shall provide confidentiality by using decryption, if necessary.	4.3.7.3.2(3)	Test	Shall	
SEC224	The downloaded software shall be checked to ensure data integrity has been maintained during the download process.	4.3.7.3.2(4)	Witness	Shall	
SEC225	The downloaded software shall be authenticated to verify it has originated from an approved source.	4.3.7.3.2(5)	Witness	Shall	
SEC226	The downloaded software shall be placed into storage (typically non-volatile BLACK storage).	4.3.7.3.2(6)	Test	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC227	The installer software shall replace the digital signature on downloaded files with an integrity check (e.g., CRC) after the digital signature has been verified and prior to placement on accessible storage.	4.3.7.3.2(7)	Test	Shall	
SEC228	The integrity and authentication of the download application software shall be verified using Type 1 cryptography.	4.3.7.3.2(8)	Inspection/ Analysis	Shall	
SEC229	The installer application shall provide the capability to install Security Policies files.	4.3.7.3.2(9)	Test	Shall	
SEC230	The installer shall use the Integrity and Authentication services of the JTRS Security API for the purpose of authenticating digitally signed files and checking their integrity.	4.3.7.3.2(10)	Witness	Shall	
SEC231	The installer shall use the Crypto services of the JTRS Security API for the purpose of encrypting and decrypting downloaded files.	4.3.7.3.2(11)	Test	Shall	
SEC232	The audit function shall operate in conjunction with alarm and exception handling within the radio.	4.3.7.4.2(1)	Test	Shall	
SEC233	The audit information shall be passed via the logger to Logger Consumers that have access restrictions for the types of events that each Consumer can collect.	4.3.7.4.2(2)	Test	Shall	
SEC234	An administrator or security officer shall be able to select the types of events that the audit function will collect and report.	4.3.7.4.2(3)	Test	Shall	
SEC235	An administrator or security officer shall be able to determine user access to the various event types.	4.3.7.4.2(4)	Test	Shall	
SEC236	The audit mechanism shall permit selection/entry of audit events by Administrators/Security Officers.	4.3.7.4.2(5)	Test	Shall	
SEC237	The audit mechanism shall examine audit record in real-time to report information on possible attacks and log for off-line analysis by system security officers.	4.3.7.4.2(6)	Test	Shall	
SEC238	The audit mechanism shall perform both event and rate driven audit functions.	4.3.7.4.2(7)	Test	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC239	The audit mechanism shall collect information on violations of the CS/S bypass security policy.	4.3.7.4.2(8)	Test	Shall	
SEC240	The audit mechanism shall collect information on violations of access control security policy.	4.3.7.4.2(9)	Test	Shall	
SEC241	The audit mechanism shall provide a delivery mechanism for logged audit records to audit personnel (infrastructure requirement).	4.3.7.4.2(10)	Test	Shall	
SEC242	The audit application shall provide for a hierarchy of audit types to support alarm and exception handling.	4.3.7.4.2(11)	Test	Shall	
SEC243	Users and protected applications shall be able to set the hierarchy of events and thresholds on auditable events to take appropriate responsive action (such as system shutdown) if an event exceeds its threshold.	4.3.7.4.2(12)	Test	Shall	
SEC244	The proper interface points within the objects of the two waveforms that are cross-banded shall be defined either within the cross-banding systems application or within the two waveform applications profiles.	4.3.7.5.2(1)	Inspection/ Analysis	Shall	
SEC245	The cross-banding application shall ensure that the cross-banding is consistent with the security policy of the affected waveforms and applications.	4.3.7.5.2(2)	Test	Shall	
SEC246	Prior to instantiation, the cross-banding application shall request a validation of security levels.	4.3.7.5.2(3)	Witness	Shall	
SEC247	Cross-banding shall only occur between applications of the same security levels.	4.3.7.5.2(4)	Witness	Shall	
SEC248	The requirements for TEMPEST will be established by individual procurements and can be found in the Unified INFOSEC Criteria (UIC)	4.4.1.1	Witness	Shall	
SEC249	The requirements for TAMPER will be established by individual procurements and can be found in the Unified INFOSEC Criteria (UIC)	4.4.2.1	Witness	Shall	
SEC250	XML files shall be derived from the relevant IDL.	4.5.2(1)	Inspection/ Analysis	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC251	NSA shall digitally sign all Security Policy XML files.	4.5.2(2)	Inspection/ Analysis	Shall	
SEC252	An XML parser shall be used to derive the required information for all policies that are used within the JTRS radio.	4.5.2(3)	Inspection/ Analysis	Shall	
SEC253	The XML parser shall calculate and append to the parsed policy an integrity checkword.	4.5.2(4)	Inspection/ Analysis	Shall	
SEC254	Policy file shall be integrity checked at instantiation.	4.5.2(5)	Inspection/ Analysis	Shall	
SEC255	Prior to the operation of a cryptographic channel, the ApplicationFactory shall send the key request to the CS/S.	4.6.1.1(1)	Not Testable	Shall	
SEC256	The CSS/S shall verify that the selected key for encryption/decryption of user data trafic (i.e., red to black, black to red) on a channel is at the same classification level as the other keys that are currently being used for encryption/decryption of user data traffic for system high applications.	4.6.1.1(2)	Witness	Shall	
SEC257	The CS/S shall verify that the selected key for encryption/decryption of information other than user/data traffic (e.g. TRANSEC, DAMA Orderwire, file encryption/decryption) is at the same classification level or below that of keys that are currently being used for encryption/decryption of user data traffic	4.6.1.1(3)	Witness	Shall	
SEC258	For system high applications, the first user traffic key instantiated into the CS/S shall be used to determine the classification and use of the radio.	4.6.1.1(4)	Witness	Shall	
SEC259	The CS/S shall either acknowledge and process the key selection request or deny the key selection request with negative acknowledgement to the user.	4.6.1.1(5)	Witness	Shall	
SEC260	All software files to be installed in the JTR shall have digital signatures attached.	4.6.2.1(1)	Inspection/ Analysis	Shall	
SEC261	The CS/S shall validate signitures prior to storage.	4.6.2.1(2)	Witness	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
SEC262	A test shall be executed that validates the correct operation of the red and black portions of the bypass individually prior to a cooperative red/black bypass test.	4.6.3.1(1)	Witness	Shall	
SEC263	A cooperative test shall execute during boot across the CS/S that tests the bypss health from the red to black.	4.6.3.1(2)	Witness	Shall	
SEC264	All waveform SW shall have an integrity check prior to instantiation.	4.6.4.1	Test	Shall	
SEC265	The Keep-Alive Ping message shall exists as part of the Security APIs.	4.6.5.1(1)	Test	Shall	
SEC266	This message shall be sent periodically between the Red GPP and the CS/S.	4.6.5.1(2)	Test	Shall	
SEC267	This message shall be sent periodically between the Black GPP and the CS/S.	4.6.5.1(3)	Test	Shall	
SEC268	Failure to receive this message from either the Red or Black GPPs shall cause to the Cryptographic to enter into an alarm state.	4.6.5.1(4)	Test	Shall	
SEC269	Operating Systems with login capability shall have logins disabled.	4.6.6.1(1)	Test	Shall	
SEC270	The OS invocation method shall be a NSA digitally signed script or an equivalent assured method.	4.6.6.1(2)	Witness	Shall	
SEC271	The script or assured method shall be validated prior to instantiation.	4.6.6.1(3)	Witness	Shall	
SEC272	The CS/S shall not permit keys to be instantiated for an improper application (e.g. Using the wrong classification key)	4.2.6.1.2.3	Witness	Shall	

SEC Tag	Requirement text	Section Number	Verification Method	Requirement Type	Change Status
Summary of Analysis					
	Not Testable		19		
	Inspection/Analy		36		
	Demonstration		0		
	Test		93		
	Witness		124		
	Total Verificatiion Method		**272**		
	Total Blank		**0**		
	Shall			272	
	Conditional			0	
	Total Requirement Type			**272**	
	Total Blank			**0**	